平成 28 年度　春期　情報セキュリティマネジメント試験　採点講評

午後試験

問 1

問 1 は，標的型攻撃メールによるマルウェア感染の脅威，従業員の情報セキュリティ意識向上策について出題した。全体として，正答率は高かった。標的型攻撃は近年大きな話題になっており，理解が進んでいたと思われる。

設問 1 では，標的型攻撃の特徴，受信者に添付ファイルを開封させる手口について問うた。(4) は，正答率が高かった。標的型攻撃メールの特徴について，よく理解されていた。

設問 2 では，標的型攻撃メールによる被害を最小化するための，規程，体制，組織文化における課題と対応について問うた。また，情報セキュリティ意識を向上させるための活動であるサイバー演習の効果を上げるための工夫について問うた。(4) は，G 君の行動の背景を分析することがポイントとなるが，正答率は平均的で，おおむね理解されていた。

標的型攻撃のように，技術的対策だけでは防ぎきれない脅威に対して，情報セキュリティリーダには，関連規程の順守状況の改善，情報セキュリティの円滑な運用に加えて，職場の情報セキュリティ文化を醸成するという役割も期待したい。

問 2

問 2 は，業務の一部を外部委託する状況での情報システムにおけるロールベースアクセス制御（RBAC）について出題した。

設問 1 は，情報システムの利用方針と業務上の要求事項の両面を踏まえ，ロールに設定する適切な操作権限を検討するという設問であり，(5)，(6) の正答率が低かった。承認手続の代行，他業務の応援といった状況においても，情報システムの利用方針及び運用上の制約を満たすことが重要である点を，是非理解しておいてほしい。

設問 2 では，社内情報の閲覧権限の付与に関する外部委託先との手続，担当者変更の際の利用者 ID 管理を問うた。(3) の正答率が高かった。業務の引継ぎという状況での適切な権限設定は，よく理解されていた。

情報システムの利用に関する内部不正を防止し，情報セキュリティを維持するために，情報セキュリティリーダには，業務で日常起こり得る変化に対して適切な権限設定を検討する役割を期待したい。

問 3

問 3 では，監査部による監査とは別に，情報システムの利用部門が主体となって行う情報セキュリティ自己点検（本問では，簡易チェック及び CSA）によってコントロールを評価する取組みについて出題した。

設問 1 は，正答率が低かった。チェック項目として，客観的に判断できる基準を明確に設定することが重要であることを理解しておいてほしい。

設問 2 では監査における CSA 方式の利点を問うたが，正答率は平均的で，おおむね理解されていた。

設問 3 は，(3) の正答率が低かった。ルールどおりに運用されていることを確認したかどうかという点が，評価する際のポイントであることを理解しておいてほしい。

設問 4 は，正答率が高かった。改善計画の策定において複数の対策を比較し検討する際には，根本的対策，暫定的対策，注意喚起などの選択肢から適切に選択することが重要だが，よく理解されていた。

情報セキュリティ自己点検は，情報システムの利用部門の情報セキュリティを効率的に維持する上で有効である。情報セキュリティリーダには，このような活動を推進する役割を期待したい。